(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2002 (10.01.2002)

PCT

(10) International Publication Number
WO 02/03290 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US01/19899

(22) International Filing Date: 22 June 2001 (22.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/598,987 22 June 2000 (22.06.2000) US

(71) Applicant: **GOPIN INC.** [US/US]; Suite 310, 1122 Kenilworth Drive, Towson, MD 21204 (US).

(72) Inventors: **SHANNON, John, P.**; 3195 Barlow Cres., R.R. 1, Dunrobin, Ontario K0A 1T0 (CA). **BOUFFARD, Claude, C.**; R.R. 1, PB/CP V4, Chelsea, Québec J0X 1N0 (CA). **SOMERVILLE, Jim, B.**; 3899A Richmond Road, Nepean, Ontario K2H 8T8 (CA).

(74) Agents: **BALDAUF, Kent, E., Jr.** et al.; Webb Ziesenheim Logsdon Orkin & Hanson, P.C., 700 Koppers Building, 436 Seventh Avenue, Pittsburgh, PA 15219-1818 (US).

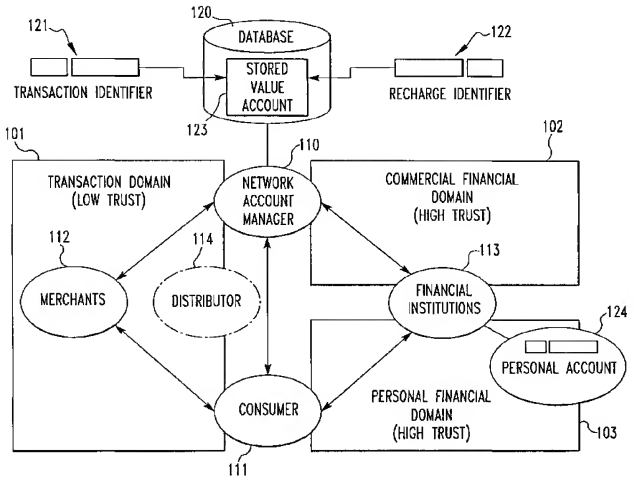
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EC, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR ANONYMOUS RECHARGING OF STORED VALUE ACCOUNTS



(57) Abstract: A system for anonymously recharging the value on telephone, gasoline, vending or other stored value accounts enables the setting up of a secondary authentication account for the subsequent application of value on the card or other instrument to conduct cash-like transactions without disclosure of personal information. When a consumer (111) wishes to add value to a depleted card or other instrument, they may communicate with a bank, credit card issuer or other financial institutions (113) to allocate an amount for recharge, which amount may then be communicated without the identity of the consumer to the account administrator. The administrator of the account in turn validates and applies this cash-like credit to the stored value instrument, thus enabling immediate recharging of the amount available on the card. No one party other than the consumer may be aware of the identity of the consumer, purchase information and other details, although transactions may be reconstructed under appropriate legal process.

WO 02/03290 A1

SYSTEM AND METHOD FOR ANONYMOUS RECHARGING OF STORED VALUE ACCOUNTS

Field of the Invention

The invention relates to the field of electronic commerce, and more particularly to a technique for replacing amounts on a stored value card or other instrument in a manner which is anonymous to some or all participants in that process, other than the card holder.

Background of the Invention

Stored value accounts, such as telephone calling cards, gas cards, duplication service cards, vending machine cards and other instruments have become a popular technique for recording and distributing commercial value. Many stored value accounts permit the card holder to freely use the amount stored on the instrument down to zero, and then permit the user to replenish the value on the card by any of a variety of techniques. For instance, the user may call an (800) number and provide a credit card or other account from which the value may be transferred to the empty stored value instrument. Similarly, a consumer who uses a stored value account to execute purchases over the Internet may enter a credit card

number or other account number to have an online card distributor place new value on their stored value account, for instance to purchase movies, records, travel or other goods or services.

However, these types of stored value recharging techniques encroach on the flexibility and privacy of the consumer. That is, while the initial purchase of the stored value card or other instrument may be anonymous, such as by purchase at a gasoline station, convenience store or other location with cash, recharging via a credit card or other authorization may not necessarily be similarly private. The recharging action therefor involves the potential exposure of sensitive credit card information to vendors or intermediaries over the Internet or otherwise.

Likewise, the recording of the recharging action on the credit card may create a permanent record of the consumer's purchase activities which the consumer may not wish to be recorded or made public. Safer, more robust technology for replenishing stored value accounts is desirable.

Summary of the Invention

The invention overcoming these and other problems in the art relates to a system and method for recharging stored value accounts via a transaction server and other infrastructure, in

which the identity of the party applying the new value to the stored value account may be anonymous to the card issuer, vendors executing purchases against that value and others in the transaction chain. According to the invention, the action of placing value on a stored value account may be separated from a vendor of goods or services, the issuer of the stored value card, and even the authentication entity providing validation of the account. In one embodiment, only the consumer and a bank or other financial institution of the consumer's choice may be aware of the consumer's identity, but under no circumstances does any party other than the consumer have sufficient information to tie together the consumer's identity, transaction identification number, the actual goods or services being purchased, bank account or other information.

Rather, separate pieces of information may be kept apart in a transaction matrix according to which no one party may discern the card holder's identity without legal permission. Privacy is therefore enhanced, and consumers may be encouraged to more freely recharge and make use of stored value accounts.

Detailed Description of the Drawings

The invention will be described with reference to the accompanying drawings, in which like elements are referenced with like numerals.

Figure 1 illustrates the principle elements according to the invention.

Figure 2 illustrates a the principle elements of the transactions involved in distribution, purchase and recharging actions for a stored value account according to the invention.

Figure 3 illustrates a matrix indicating the availability of transaction information to parties to the recharging action of the invention.

Figure 4 illustrates an overall architecture for transaction processing according to the invention.

Figure 5 illustrates an overall architecture for transaction processing according to the invention in another regard.

Detailed Description of Preferred Embodiments

As illustrated in Figures 1 and 4, in an overall electronic commerce environment in which the invention may operate, a customer or consumer operating an Internet or other client 111 communicates via communication link 401 to one or more of a group of merchants 112 to execute transactions using

a stored value account identifier 121 as the method of payment. The stored value account identifier 121 may be or include an alphanumeric reference to a database, a telephone calling card, a vending card, a gasoline card, a frequent flier or other account, card or instrument representing commercial value and in general may be anonymously recharged, in general via a separately maintained account identifier 122.

The client 111 in the environment may be or include, for instance, a personal computer running the Microsoft Windows™ 95, 98, Millenium™, NT™, or 2000, Windows™CE™, PalmOS™, Unix, Linux, Solaris ™, OS/2 ™, BeOS ™, MacOS ™ or other operating system or platform. The client 102 may also be or include a network-enabled appliance such as a WebTV™ unit, radio-enabled Palm™ Pilot or similar unit, a set-top box, a networkable game-playing console such as Sony Playstation™ or Sega Dreamcast™, a browser-equipped cellular telephone, or other TCP/IP client, a magnetic swipe-card reader connected to a network via the Internet or a modem, a point of sale terminal, or other device.

The communications link 401 to which client 111 is connected may be, include or interface to any one or more of, for instance, the Internet, an intranet, a PAN (Personal Area Network), a LAN (Local Area Network), a WAN (Wide Area Network) or a MAN (Metropolitan Area Network), a frame relay

connection, an Advanced Intelligent Network (AIN) connection, a synchronous optical network (SONET) connection, a digital T1, T3 or E1 line, Digital Data Service (DDS) connection, DSL (Digital Subscriber Line) connection, an Ethernet connection, an ISDN (Integrated Services Digital Network) line, a dial-up port such as a V.90, V.34 or V.34bis analog modem connection, a cable modem, an ATM (Asynchronous Transfer Mode) connection, or FDDI (Fiber Distributed Data Interface) or CDDI (Copper Distributed Data Interface) connections. The communications link 401 may furthermore be, include or interface to any one or more of a WAP (Wireless Application Protocol) link, a GPRS (General Packet Radio Service) link, a GSM (Global System for Mobile Communication) link, a CDMA (Code Division Multiple Access) or TDMA (Time Division Multiple Access) link such as a cellular phone channel, a GPS (Global Positioning System) link, CDPD (cellular digital packet data), a RIM (Research in Motion, Limited) duplex paging type device, a Bluetooth radio link, or an IEEE 802.11-based radio frequency link. The communications link 401 may yet further be, include or interface to any one or more of an RS-232 serial connection, an IEEE-1394 (Firewire) connection, an IrDA (infrared) port, a SCSI (Small Computer Serial Interface) connection, a USB (Universal Serial Bus) connection or other wired or wireless,

digital or analog interface or connection. Other illustrated communications links may include the same types of resources.

The communications like 401 and other communications link described herein may employ security measures as desired, such as by public key encryption techniques, e.g. Secure Socket Layer (SSL) via the Internet, DES or other measures.

In the illustrated embodiment, including as illustrated in Figure 4, other communications resources may include communications link 410, which may connect a consumer or user to a bank or other financial institution, such as by any of the above Internet protocols or via an ATM, deposit slip, personal check, wire transfer or any other acceptable funds transfer mechanism.

The communications link 402 may connect the merchant or vendor to the network, and the communications link 403 may connect the consumer to the via a point of sale terminal such as those used for debit card transactions. The communications links 411, 412 may connect participating banks to banks, a bank to a business and may be or employ virtual private networks, wire transfer or other techniques.

The communications links 433, 434, 435 may be physical or may be software database, logical or memory linkages in the case that all functions are integrated in certain implementations. The communications link 435 may be or

interface to the common channel signaling number 7 (CCS#7) protocol. The communications links 441, 442 may involve non-electronic transfer of physical goods (e.g. plastic or paper cards), or may involve electronic transfer of information.

The vendor or vendors 112 communicate with the network account manager 110 sub-element transaction server 421 via communication link 402, to prepare transaction information for recording and collection. The transaction server 421 may be or include, for instance, a workstation running the Microsoft Windows™ NT™, Windows™ 2000, Unix, Linux, Xenix, IBM AIX, Hewlett-Packard UX, Novell Netware™, Sun Microsystems Solaris™, OS/2™, BeOS™, Mach, Apache, OpenStep™ or other operating system or platform. The transaction server 421 is in turn connected and acts as a front end resource to the stored value account database 120 via communications link 431.

The stored value account 120 in turn may consist of a network of database functions, shown separately as three discrete elements, namely the recharge database network 422 (indexed by Recharge ID 122), the stored value account database network 423 which provides an association between recharge ID 122 and transaction ID 121, and the transaction authentication database network 424, (indexed by transaction ID 121).

The stored value account database network 424 may be or include a Nortel Networks DMS™ 100, 200, 300 or other series hardware dedicated to switching and processing telecommunications resources, and may furthermore be or include, for instance, a workstation running the Microsoft Windows™ NT™, Windows™ 2000, Unix, Linux, Xenix, IBM AIX, Hewlett-Packard UX, Novell Netware™, Sun Microsystems Solaris™, OS/2™, BeOS™, Mach, Apache, OpenStep™ or other operating system or platform. The network interface 422 itself communicates via communications link 432 with network database 120 for purposes of transaction validation.

The transaction authentication database network 424 may be, include or interface to a line information data base (LIDB)-type resource operating under the SS7 signaling standard and accessible in the public telecommunications network, as understood by persons skilled in the art, for purposes of authentication, authorization or other transaction functions against a stored value calling card, vending card or other stored value account identifier 121. Transaction authentication database network 424 may likewise be, include or interface to resources such as the ATT Corp. Billing Validation Application (BVA) or the U.S. West Business Validation Service (BVS), or others. The authentication database 110 may further be, include or interface to, for

example, the Oracle™ relational database sold commercially by Oracle Corp. Other databases, such as Informix™, DB2 (Database 2) or other data storage or query formats or platforms such as OLAP (On Line Analytical Processing), SQL (Standard Query Language), Microsoft Access™ or others may also be used, incorporated or accessed in the invention.

The recharge database network 422 may be or include similar resources as the transaction authentication database network 424, configured to manage the bank or other financial accounts, or a database of such accounts, maintained by or on behalf of the network account manager 110 for replenishment of the stored value accounts.

In general, according to the invention the stored value account 123 to be offered in payment for transactions with the merchants 112 using transaction identifier 121 may be rechargeable by transferring value from another account or resource using recharge identifier 122. Transaction identifier 121 may be or include multi-part keys, consisting of a public identifier such as an account number and a secret private identifier such as a PIN, or otherwise according to a variety of available schemes for authenticating the usage of an ID over an insecure public infrastructure.

The recharge identifier 122 may bear no relationship to the transaction identifier 121, or it may consist in whole or

in part of the transaction identifier or a subset or permutation thereof. Furthermore, recharge identifier 122 may identify a bank account number, a checking account number, a credit card number, customer account number, a direct deposit number, an automatic bill pay number or other identifier which can be readily processed as a deposit identifier by the financial industry.

In terms of the action of obtaining the instrument, as illustrated in Figure 2, in action 211 the network account manager 110 creates an individual account 123a consisting of a unique transaction identifier 121a associated with a unique recharge identifier 122a. The network account manager 110 may optionally associate a non-zero account balance with the initially created account, as is often done with prepaid telephone cards for example.

The network account manager 110 may distribute accounts to consumers 111 directly, or may optionally engage the services of a distributor 114. Assuming the general aspect where a distributor is engaged, the network account manager 110 provides the account information to the distributor 114 in transaction 202 according to any number of mechanisms such as are currently used for the distribution of prepaid telephone cards. A customer 111a may obtain the account from the distributor 114 in transaction 203, without providing an

opportunity to have their identity associated with the transaction ID 121a or the recharge identifier 122a. There are a variety of methods for achieving this security. For example, the consumer might obtain a card containing the information from a vending machine, or they might purchase a card from a retail store, which card has secret information concealed from the vendor. Or, the consumer might obtain the information via an Internet, telephone dial-up or other communication connection, or via mass market distribution such as in cereal boxes, with CD's or as magazine inserts.

Optionally, as shown in transaction 204, the consumer 111a may be required or given the capability to activate the instrument, or charge up the instrument for the first time, and/or change any or all of the ID information.

It may be noted that the activities provide a mechanism where a consumer 111a may obtain a stored value account 123a identified to them as consisting of a transaction ID 121a and a recharge identifier 122a such that they do not reveal their identity to the network account manager 110. Further, these activities also provide that the distributor is unable to associate the consumer's identity 111a with the transaction ID 121a or the recharge identifier 122a, even if the distributor knows the identity of the consumer (solved by concealing the Ids from the distributor), or if the distributor knows the Ids

(solved by the consumer acquiring the account without revealing their identity), or both (solved by allowing the consumer to change the IDs).

In terms of the purchasing action, as shown in Figure 2, an individual consumer 111a may engage with an individual merchant 112a to initiate a purchase request in communication 211. At least two embodiments of this communication are possible. In a first embodiment, the consumer discloses transaction ID 121a to the merchant in communication 211, such as is the case with credit card purchases today. The merchant subsequently initiates communication 212a with the network account manager 110, which queries the authentication elements of network database 120 and authenticates the transaction ID 121a, provides validation that account 123a can make good on the purchase price, confirms authentication to the merchant in communication 212c, posts a debit to the account maintained in network database 120 in action 213 and remits payment to the merchant in communication 215, which payment may occur immediately or substantially later.

Having received confirmation in communication 212c, the merchant 112a provides the goods to consumer 111a in communication 214. This embodiment may pose a potential security issue in that the merchant may fraudulently use or distribute the transaction ID 123a. In a preferred

embodiment, the consumer 111a does not disclose the transaction ID to the merchant in communication 211. Instead, the in communication 212a the merchant 112a redirects an authorization request including the amount of purchase to the network account manager 110, who then engages communication 212b with the consumer 111a directly. Consumer 111a provides transaction information 121a only to the network account manager, who subsequently informs the merchant 112a of successful authorization via communication 212c. The remaining actions and communications 213 through 215 remain the same as in the first embodiment. Hybrid embodiments similar to today's debit cards are also possible, where the merchant or vendor is presented with a portion of the transaction ID 121a (the debit card number), and the consumer provides the rest of the transaction ID 121a (the PIN) to the network account manager 110 in order to complete the authorization.

In the course of providing the goods or services provided, merchant 112a may interact or communicate with other merchants, suppliers or distributors, and may subsequently remit to them a portion of the payment received from the consumer via the network account manager, which communications are not shown for clarity.

In this purchase activity, it may be noted that consumer's identity 111a is not required to be revealed to either the merchant 112a nor the network account manager 110, and that at most the merchant may learn of the consumer's transaction ID 121a, or a portion thereof. Furthermore, the network account manager 110 is not necessarily made aware of the goods or services provided by the merchant 112a to the consumer 111a.

In terms of the recharging action, as illustrated in Figure 2, the financial institution 113a may by prearrangement maintain checking, credit, deposit or other accounts on behalf of the consumer 113a, from which the consumer may recharge their stored value account 123. In communication 221, the consumer 111a authenticates themselves to the satisfaction of the financial institution.

In communication 222 the consumer 111a may transmit a signal to or otherwise request financial institution 113a to debit their bank or other account in order to apply new value to the stored value account 122 maintained by or for the network account manager 110. If financial institution 113a determines that the amount presented for debit is valid, financial institution 113a may issue a communication 224 to the network account manager or its representative with an instruction to credit the consumer's authentication account

122 by that same amount. The network account manager thus receives communication 224 to increase the consumer's authentication account 130, without any necessary indication of the identity of the consumer.

Indeed, it is not necessary that the consumer recharging the account 120 through the recharge identifier 122 be the user of transaction account 121. It may be noted that for the recharge operation neither the optional distributor 114, nor the merchant 112 receives any information concerning recharge identifier 122. Furthermore, the financial institution does not receive any information concerning the transaction identifier 121.

While the network account manager must receive both identifiers 121 and 122, and jointly associates them with account 123, nothing in the recharge operation provides the network account manager with the identity of consumer 111a.

As illustrated in Figure 3, the interposition of a transaction server 421 for transaction purposes with the network interface entity 422 and network database cooperating as the network account manager 110, along with financial institutions 113 and other elements results in increased security and privacy to the consumer performing the recharging action on their stored value account 123. As shown in the

transaction matrix of Figure 3, only the consumer 111a is in possession of all categories of information involved in the use and recharging of the stored value account 120, including the consumer's identity, any transaction ID (such as sales receipt number, purchase order number or other), the identity of the goods or services purchased, the bank deposit identification, and the bank account identification or other information surrounding the replenishment of stored value or the purchase of goods or services using that value.

Thus, the distributor 114, as shown in that matrix, may not be aware of any of those categories of information (except perhaps the identity of their consumers, but not what they purchase or details of their financial situation). Similarly, the network account manager 110 is only necessarily aware of the transaction ID and the recharge ID.

The merchants are only aware of the goods and services they have provided, and possibly some or all of the transaction ID (except in a preferred embodiment where they do not possess this information). Financial institutions 113 such as a bank or credit card issuer may only be aware of the consumer's identity along with the internal banking information such as bank deposit ID and bank account ID.

The network account manager 110 learns the transaction ID associated with the purchase or other transaction, along with

the bank deposit ID, in order to properly credit the stored value account 123 by way of debit from the financial institution to show account. However network database 120 is not made aware goods or services purchased since this information is masked by the transaction server 421 and is not necessary in the communication between transaction server 421 and network interface 422.

At the same time, according to the invention the combination of two or more sources of information among the stored value account issuer 204, financial institution 206, vendor 208 and authentication entity 210 may provide sufficient linkage to derive the identity of the consumer, the identity of the goods or services purchased or other information when legally necessary and appropriate, such as by means of a valid subpoena or other inquiry for investigative purposes.

However, during ordinary circumstances there is no mechanism for any party other than the consumers 111 to be aware of the entire recharging and transaction activities, so that their overall privacy and security is enhanced. Moreover, the commercial convenience of vendors 112 is increased, since the validation of the transaction against an authenticated stored value account 123 creates a more cash-like basis for online or other commerce.

A further aspect of the invention is that the stored value account 123 is preferably instantiated as a network database 120, which may consist of two or more distinct databases (or networks of databases). This network database performs at least three functions: firstly, authentication of a transaction ID 121; secondly, maintaining the balance of funds on account, identified by recharge ID 122, and thirdly reconciling between these two functions. For example, the first function may be performed using an authentication database maintained in one part of the network database (such as a telephone calling card account) indexed by the transaction ID 121, which could be a calling card number and PIN.

The second function could represent a set of bank accounts or credit card numbers, maintained in another part of the network database, possibly by a financial institution, indexed by the recharge ID. The third function might be a relational database associating the transaction ID bi-directionally with a customer number not necessarily related to the identity of the customer, and the recharge ID with the corresponding customer number, also bi-directionally. These parts of the network database may be owned and operated by different cooperating parties - for example, by financial institutions providing deposit facilities and by telephone

companies providing authentication and billing facilities, and by service bureaus providing the linkage. Such an implementation provides that an efficient network of both credit and debit facilities may be constructed using existing networks of authentication and billing systems (such as the telephone billing system) without modification.

In another regard, a network account manager may wish to permit the value of the stored value of the account to a given consumer to decrease below zero value (or possibly to a limit) in affect creating a temporary credit account, depending on terms of the account and the nature of consumer 202.

While execution of a transaction according to the invention thus requires the intervention of more parties then with conventional card recharging, privacy is significantly increased while still permitting reconstruction of given transactions for valid purposes.

An overall architecture according to the invention in another regard is illustrated in Figure 5, in which the interconnection of a transaction server 206, a telephony engine 208 such as the Nortel Networks DMS™ platform for interface to the telecommunications network for authentication and billing and other services, the vendor transaction site or sites such as Web pages or other portals, the client and other aspects are shown.

In general, according to the overall architecture in which the invention in one embodiment may operate, consumers may initiate and execute transactions over a dial-up, broadband or other Internet or other network connections, which transactions may be monitored and mediated via transaction server 206, a telephony engine 208 or other network interface along with attendant database, communications and other resources. The messaging traffic between the consumer and the vendor, and between the vendor and the authentication resources, again may be of a partial, anonymous and/or secure nature.

This is at least in part because the invention does not demand the transmission of complete identity or account information, whether in the clear, encrypted or otherwise, at any one stage of the transaction process. Rather, a subset of selected attributes, fields or keywords may be queried between the consumer and the commercial vendor for the separate transmission to the party, company or other organization operating the transaction server 206, telephony engine 208 or other network interface, or authentication database 210, and only the party providing the authentication function necessarily records more complete information in order to carry out that task. As shown in that figure and described above, billing against the consumer's account, telephone bill

or otherwise may be triggered by a validated authentication sequence whose details may never be communicated to the vendor. The vendor may consequently receive payment directly or indirectly from banks or other financial intermediaries separately after that process, with whom the consumer separately reconciles. Transaction privacy and flexibility for consumers are therefore enhanced.

The foregoing description of the system and method of the invention is illustrative, and variations in configuration and implementation will occur to persons skilled in the art.

For instance, while the recharging cycle has generally been described as taking place between entities including a financial institution 113, a Web or other vendor 112 and an network account manager 110, different of these functions may be divided amongst other entities and resources, or likewise combined in certain implementations. For example, the functions of the network account manager could be performed by a service bureau, a telephone company (authentication & transaction billing), and a bank (payment & recharge). Likewise, while the stored value account has been described in terms of discrete parts (transaction ID, recharge ID) in terms of separate accounts, the stored value account 123, transaction ID 121 and recharge ID 123 could either be a

subset, a superset or co-extensive set with each other, or represent multiple accounts.

Similarly, while the invention has generally been described with respect to the stored value card initially coded with some amount of value, the invention may also be applied to stored value accounts whose initial balance is zero, or which is allowed to remain below zero for a period of time and periodically recharged, not necessarily to a positive balance. While the invention has generally been described as recharge of the stored value account being initiated by actions of the consumer, it is possible that the consumer may be prompted to recharge the account by presentment of a bill for any negative value. Although the invention has been described as though the value is a financial currency, it generally applies for other value systems such as loyalty points and so on, and the term "financial institution" is intended to generally represent providers or holders of value whether currency or otherwise. Translation between different types of value may also be possible. The scope of the invention is accordingly intended to be limited only by the following claims.

What is claimed is:

1. A system for the anonymous recharging of a stored value account, comprising:

a first interface to a stored value account;

a second interface, communicating with the first interface, to an anonymous authentication account;

a third interface to a financial account held by an account holder, communicating with the first interface to apply value from the financial account to the stored value account upon instruction of the holder of the financial account;

wherein the stored value account is recharged by the value delivered via the third interface, and the anonymous authentication account is reduced by the value communicated via the second interface.

2. The system of claim 1, wherein the stored value account comprises at least one of a telephone calling card account, a vending card account, a duplication card account, a gasoline card account, a private label account, and a frequent flier account.

3. The system of claim 1, wherein the financial account comprises at least one of a checking account, a debit account, a deposit account, and a credit account.

4. The system of claim 1, further comprising a fourth interface, communicating with a transaction site, a transaction being executed at the transaction site via the fourth interface using the stored value account.

5. The system of claim 4, wherein the transaction site comprises an Internet-enabled transaction site.

6. The system of claim 4, wherein only the account holder has access to information related to all of the stored value account, the financial account, the anonymous authentication account and the transaction.

7. The system of claim 1, wherein at least one of the stored value account, the financial account and the anonymous authentication account comprises a subset of the remainder of the stored value account, the financial account and the anonymous authentication account.

8. The system of claim 1, wherein at least one of the stored value account, the financial account and the anonymous authentication account comprises a superset of the remainder of the stored value account, the financial account and the anonymous authentication account.

9. The system of claim 1, wherein at least one of the stored value account, the financial account and the anonymous authentication account comprises a coextensive set with the

remainder of the stored value account, the financial account and the anonymous authentication account.

10. The system of claim 1, wherein the stored value account may store a value less than zero.

11. The system of claim 1, wherein the anonymous authentication account is provided by the telecommunications network.

12. The system of claim 1, wherein the recharging is via at least one of automatic bill payment and direct deposit.

13. The system of claim 1, wherein the transaction is conducted with reference to a stored value account indicator, which a network account manager translates to transaction ID and authenticates.

14. A method for the anonymous recharging of a stored value account, comprising the steps of:

a) communicating instructions to a financial institution to deliver value by deposit to a recharging account;

b) recharging the stored value account by the value delivered from the financial institution;

wherein the account to which funds are deposited is maintained for the purpose of recharging the stored value account, and where the recharging account is associated with the stored value account.

15. The method of claim 14, wherein the stored value account comprises at least one of a telephone calling card account, a vending card account, a gasoline card account, a private label account, a duplication card account, and a frequent flier account.

16. The method of claim 14, wherein the financial account comprises at least one of a checking account, a debit account, a deposit account, and a credit account.

17. The method of claim 14, further comprising a step of c) executing a transaction on a transaction site using the stored value account.

18. The method of claim 17, wherein the transaction site comprises an Internet-enabled transaction site.

19. The method of claim 17, wherein only the account holder has access to information related to all of the stored value account, the financial account, the anonymous authentication account and the transaction.

20. The method of claim 14, wherein at least one of the stored value account, the financial account and the anonymous authentication account comprises a subset of the remainder of the stored value account, the financial account and the anonymous authentication account.

21. The method of claim 14, wherein at least one of the stored value account, the financial account and the anonymous

authentication account comprises a superset of the remainder of the stored value account, the financial account and the anonymous authentication account.

22. The method of claim 14, wherein at least one of the stored value account, the financial account and the anonymous authentication account comprises a coextensive set with the remainder of the stored value account, the financial account and the anonymous authentication account.

23. The method of claim 14, wherein the stored value account may store a value less than zero.

24. The method of claim 14, wherein the anonymous authentication account is provided by the telecommunications network.

25. The method of claim 14, wherein the recharging is via at least one of automatic bill payment and direct deposit.

26. The method of claim 14, wherein the transaction is conducted with reference to a stored value account indicator, which a network account manager translates to transaction ID and authenticates.

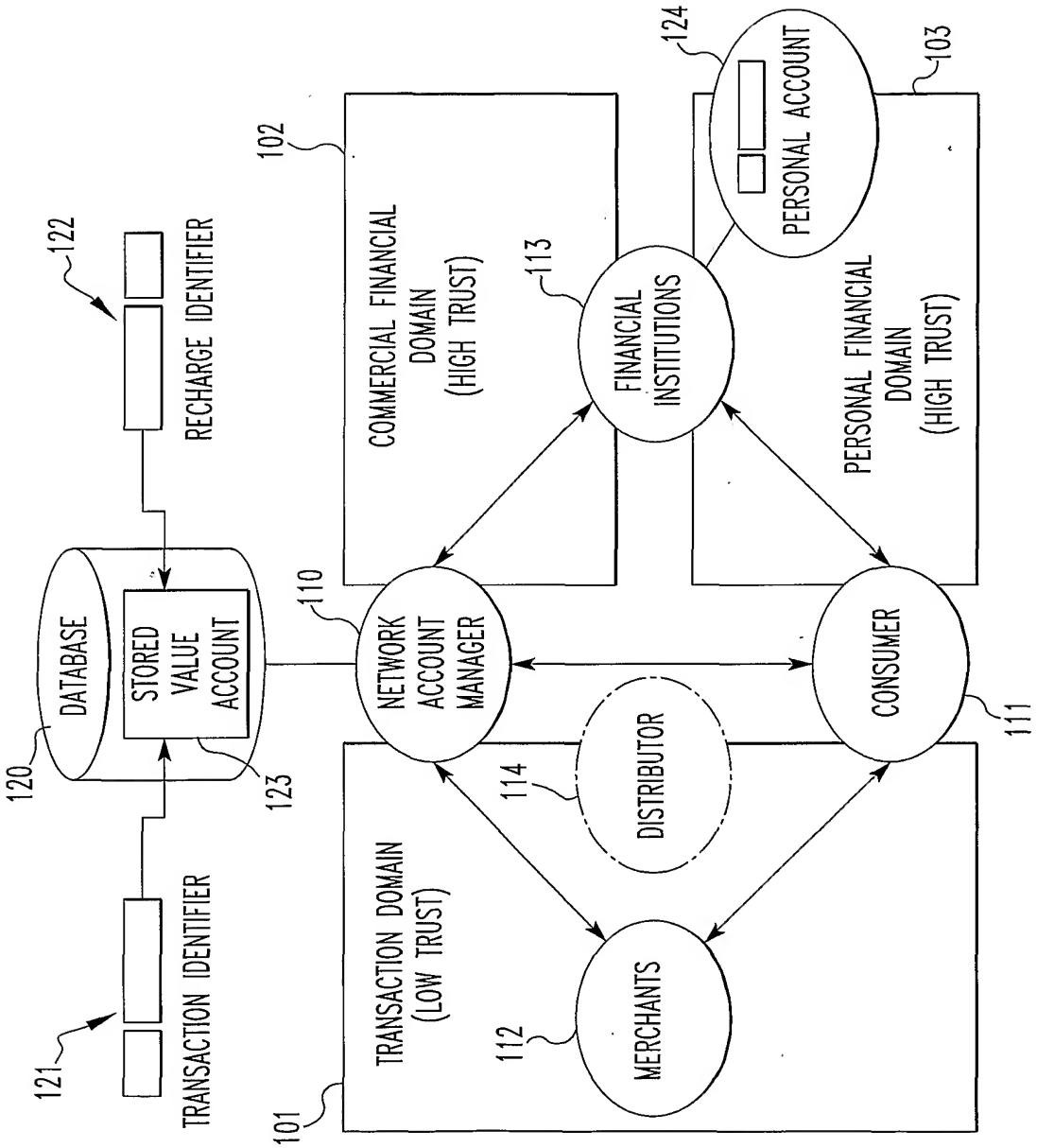

122
RECHARGE IDENTIFIER
102
COMMERCIAL FINANCIAL DOMAIN (HIGH TRUST)
113
FINANCIAL INSTITUTIONS
124
PERSONAL ACCOUNT
103
PERSONAL FINANCIAL DOMAIN (HIGH TRUST)
DATABASE
STORED VALUE ACCOUNT
110
NETWORK ACCOUNT MANAGER
CONSUMER
111
120
123
114
DISTRIBUTOR
TRANSACTION DOMAIN (LOW TRUST)
112
MERCHANTS
101
121
TRANSACTION IDENTIFIER

FIG. 1

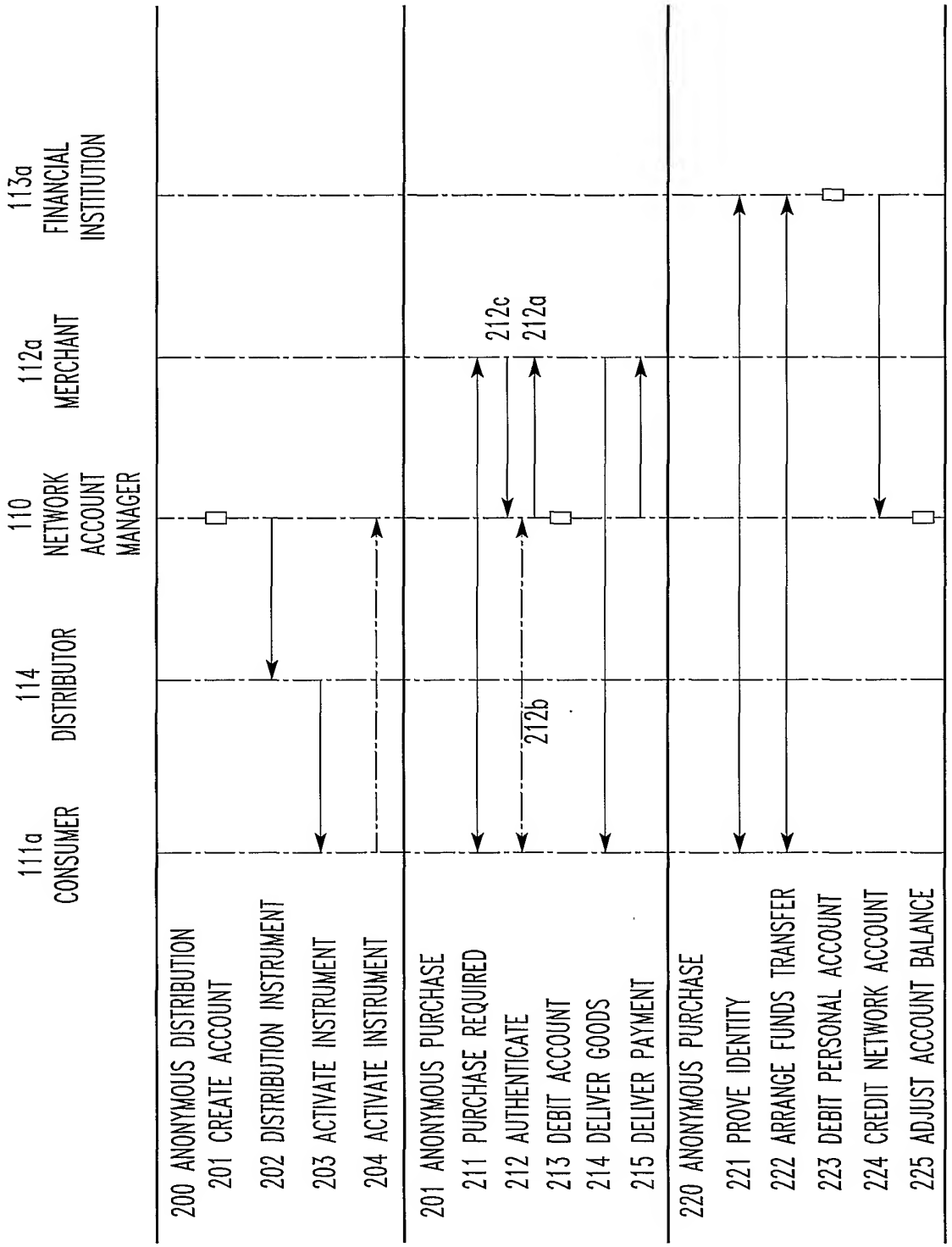

111a CONSUMER
114 DISTRIBUTOR
110 NETWORK ACCOUNT MANAGER
112a MERCHANT
113a FINANCIAL INSTITUTION
200 ANONYMOUS DISTRIBUTION
201 CREATE ACCOUNT
202 DISTRIBUTION INSTRUMENT
203 ACTIVATE INSTRUMENT
204 ACTIVATE INSTRUMENT
201 ANONYMOUS PURCHASE
211 PURCHASE REQUIRED
212 AUTHENTICATE
213 DEBIT ACCOUNT
214 DELIVER GOODS
215 DELIVER PAYMENT
212c
212a
212b
220 ANONYMOUS PURCHASE
221 PROVE IDENTITY
222 ARRANGE FUNDS TRANSFER
223 DEBIT PERSONAL ACCOUNT
224 CREDIT NETWORK ACCOUNT
225 ADJUST ACCOUNT BALANCE

FIG.2

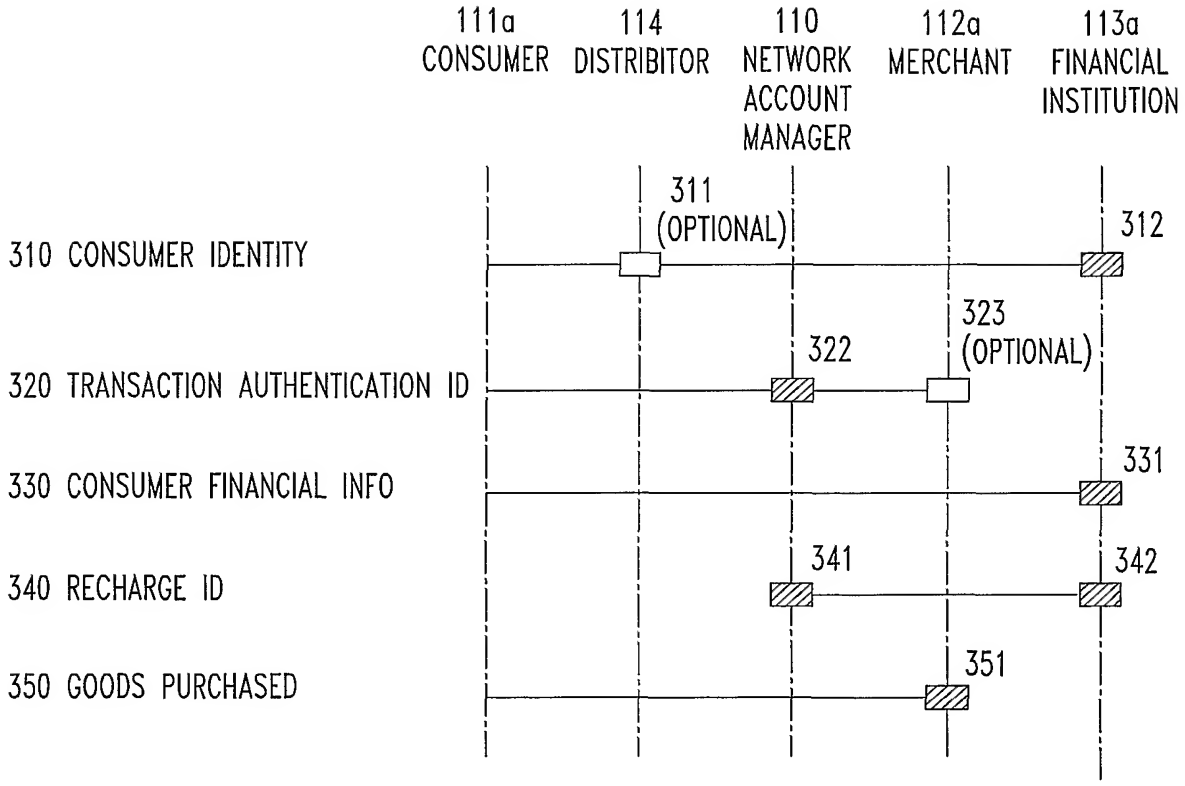

111a
CONSUMER
114
DISTRIBITOR
110
NETWORK
ACCOUNT
MANAGER
112a
MERCHANT
113a
FINANCIAL
INSTITUTION
311
(OPTIONAL)
312
310 CONSUMER IDENTITY
323
(OPTIONAL)
322
320 TRANSACTION AUTHENTICATION ID
331
330 CONSUMER FINANCIAL INFO
341
342
340 RECHARGE ID
351
350 GOODS PURCHASED

FIG.3

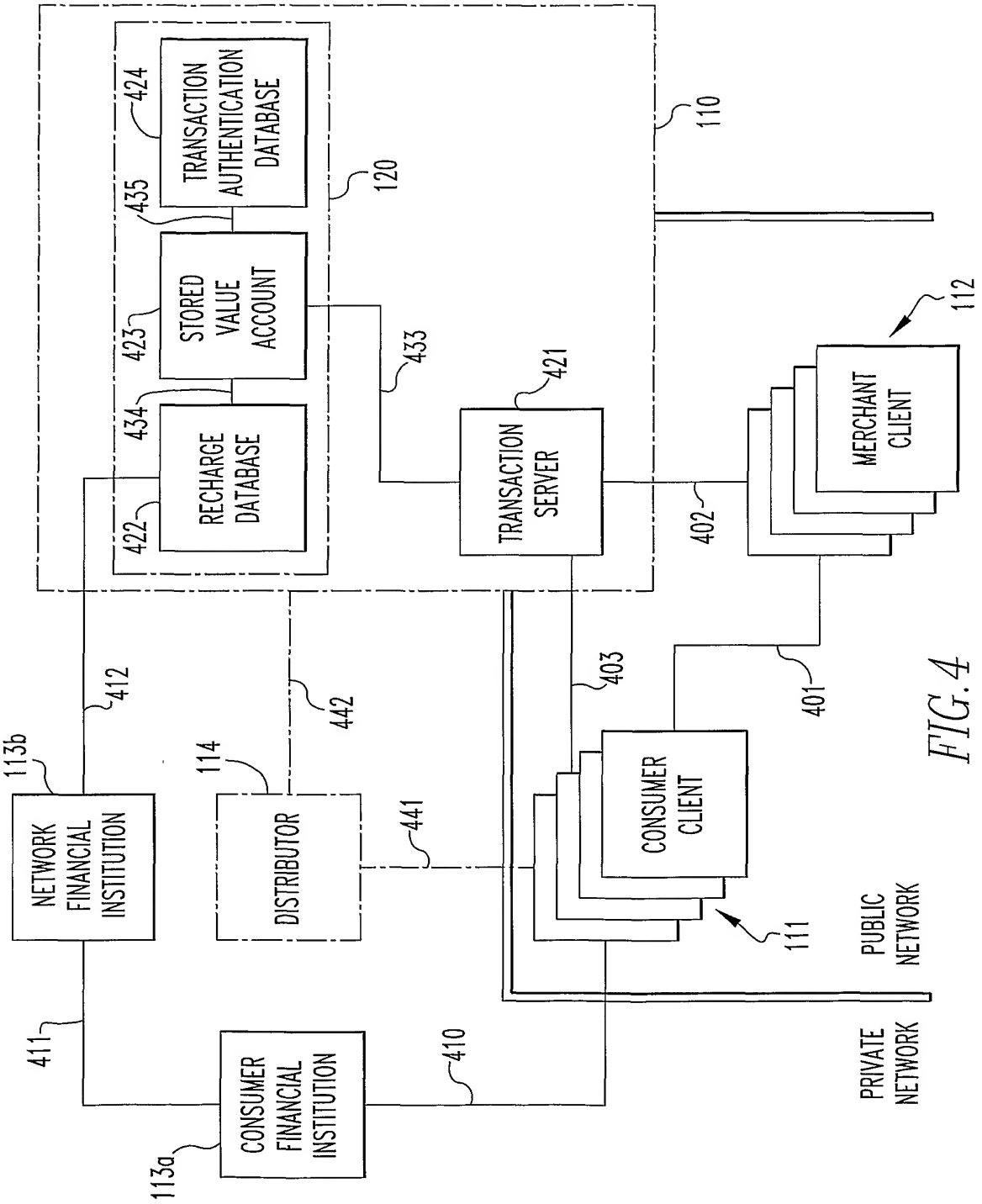
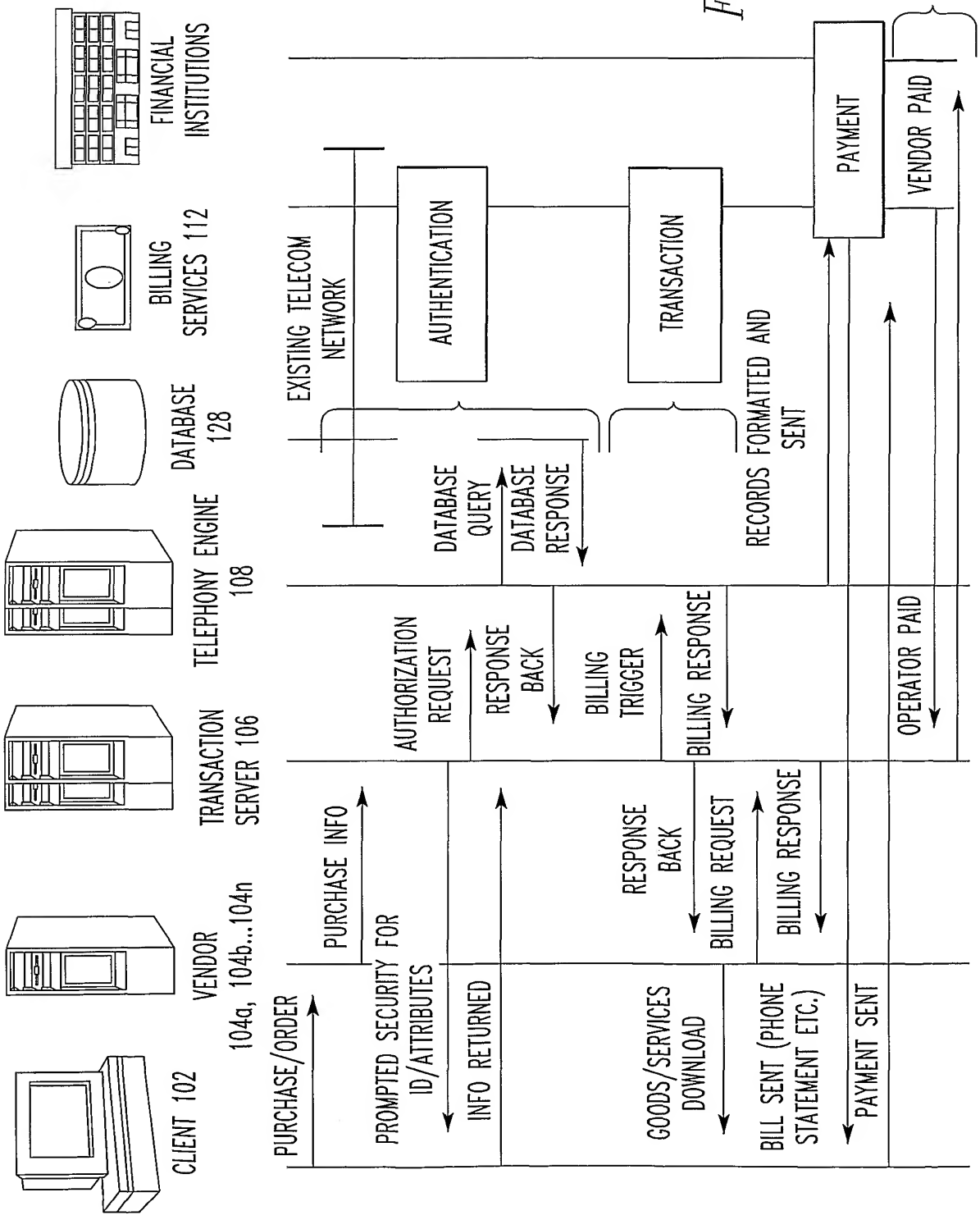

TRANSACTION AUTHENTICATION DATABASE
424
435
STORED VALUE ACCOUNT
423
434
RECHARGE DATABASE
422
120
110
433
TRANSACTION SERVER
421
MERCHANT CLIENT
112
402
412
442
403
401
113b
NETWORK FINANCIAL INSTITUTION
114
DISTRIBUTOR
441
CONSUMER CLIENT
111
PUBLIC NETWORK
411
CONSUMER FINANCIAL INSTITUTION
410
113a
PRIVATE NETWORK

FIG. 4

FIG.5


CLIENT 102
VENDOR 104a, 104b...104n
TRANSACTION SERVER 106
TELEPHONY ENGINE 108
DATABASE 128
BILLING SERVICES 112
FINANCIAL INSTITUTIONS
EXISTING TELECOM NETWORK
AUTHENTICATION
TRANSACTION
PAYMENT
VENDOR PAID
PURCHASE/ORDER
PURCHASE INFO
PROMPTED SECURITY FOR ID/ATTRIBUTES
INFO RETURNED
AUTHORIZATION REQUEST
RESPONSE BACK
DATABASE QUERY
DATABASE RESPONSE
BILLING TRIGGER
BILLING RESPONSE
RECORDS FORMATTED AND SENT
RESPONSE BACK
GOODS/SERVICES DOWNLOAD
BILLING REQUEST
BILLING RESPONSE
BILL SENT (PHONE STATEMENT ETC.)
PAYMENT SENT
OPERATOR PAID

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/19899

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G 06 F 17/60
US CL : 705/44

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/44

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

east, west, dialog

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,963,647 A (DOWNING et al) 05 October 1999, fig. 2,3,5A,5B,6. col. 3, lines 40-51. col. 14, lines 21-54.	1-26
Y	US 6,014,646 A (VALLEE et al) 11 January 2000, abstract, col. 1, lines 1-29, 52-64. col. 2, lines 33-61. col. 5, lines 17-50.	1-26
A	US 6,064,990 A (GOLDSMITH) 16 May 2000, abstract, fig 1, 4. col. 3, lines 48-57.	1-26
A	US 6,078,902 A (SCHENKLER) 20 June 2000, abstract, fig. 6. lines 7-49.	1-26
A	US 6,062,472 A (CHEUNG) 16 May 2000, abstract. fig. 3A,3B. col. 2, lines 9-26.	1-26

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search

22 AUGUST 2001

Date of mailing of the international search report

14 SEP 2001

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

VINCENT MILLIN

Telephone No. (703) 308-1065

Form PCT/ISA/210 (second sheet) (July 1998) ★